					Insert Registered Legal Entity Name Here							
Document number: P13					Document Title: **Data Classification and Labeling Policy**							
Version: 1.0		Effective Date: 01.01.2025			Document Owner:							
X	Policy		Standard		Procedure		Form		Register		Other	

Revision history				
Revision number	**Revision Date**	**Changes**	**Reviewed by**	**Process owner**

Approvals			
Name	**Title**	**Date**	**Signature**

1. Purpose

1.1 This policy establishes the formal framework for classifying and labeling organizational information assets based on sensitivity, risk exposure, and regulatory obligations.

1.2 It ensures that all information—whether stored, transmitted, or processed—is clearly categorized and labeled in a manner that communicates the required level of protection and handling.

1.3 This policy mandates structured classification aligned with the organization's Risk Management Policy, supporting Confidentiality, Integrity, and Availability objectives across both digital and physical data types.

1.4 This control is essential to enable role-based access, audit readiness, appropriate data sharing, and the effective implementation of technical controls such as encryption, backup, and monitoring and threat detection.

2. Scope

2.1 This policy applies to:

2.1.1 All organizational information assets, including documents, databases, records, and communications

2.1.2 All data formats, including digital, printed, written, and verbal

2.1.3 All environments, including on-premises, remote access, mobile, and cloud

2.1.4 All employees, contractors, service providers, and third-party processors who create, handle, or store organizational information

2.2 The scope includes internally developed content, externally sourced data, personal data subject to data privacy law obligations (e.g., GDPR), and information exchanged with clients, partners, and regulators.

2.3 It applies to all systems used to store or transmit data, including enterprise applications, file servers, email systems, cloud platforms, and backup repositories.

3. Objectives

3.1 To establish a standardized, organization-wide classification scheme based on the impact of data exposure or compromise.

3.2 To ensure all information is visibly and persistently labeled to reflect its classification level and data handling requirements.

3.3 To enforce data handling and access controls aligned with classification, including encryption, logging, transmission protection, and retention scheduling.

3.4 To support compliance with international standards (ISO/IEC 27001, 27002), legal frameworks (GDPR, NIS2, DORA), and internal risk policies.

3.5 To ensure that all users understand their responsibilities for protecting data, applying labels, and handling classified information correctly.

3.6 To maintain traceability between classification status, associated controls, and the organization's asset inventory for audit and compliance purposes.

4. Roles and Responsibilities

4.1 Chief Information Security Officer (CISO)

4.1.1 Owns this policy and ensures alignment with regulatory, contractual, and operational requirements.

4.1.2 Approves classification levels, labeling standards, and policy revisions.

4.1.3 Oversees compliance with this policy through IT audits, metrics, and exception reviews.

4.1.4 Coordinates with Legal and Compliance, Data Privacy, and risk management teams.

4.2 Information Owners

4.2.1 Are responsible for classifying information assets under their control using the organizational classification schema.

4.2.2 Apply classification labels at the time of creation, update, or intake.

4.2.3 Periodically review asset classification, particularly in response to changes in sensitivity, regulatory scope, or business value.

4.2.4 Ensure that sensitive data is handled and labeled appropriately throughout its information asset lifecycle.

[... Sections 4.3–8 are not included in this preview. Purchase the full document to access the complete policy content. ...]

9. Review and Update Requirements

9.1 This policy shall be reviewed at least annually to ensure alignment with:

9.1.1 Evolving regulatory requirements (e.g., GDPR, NIS2, DORA)

9.1.2 Updates to ISO/IEC 27001 or ISO/IEC 27002 classification guidance

9.1.3 Organizational changes affecting data sensitivity or ownership

9.1.4 Technological changes, including new document or data management platforms

9.2 The Chief Information Security Officer (CISO) shall initiate the review in collaboration with the Information Security Committee, Legal Counsel, and affected business units.

9.3 Reviews shall include:

9.3.1 Effectiveness of classification enforcement and user adherence

9.3.2 Analysis of incidents or exceptions related to misclassification

9.3.3 User feedback on labeling tools or guidance materials

9.3.4 Benchmarking against industry classification standards

9.4 Policy updates must be version-controlled, documented in the ISMS Document Repository, and communicated to all relevant personnel, with emphasis on new responsibilities or tool changes.

9.5 New hires must be introduced to the current version of the policy during onboarding. All employees must complete annual refresher training following significant policy changes.

10. Related Policies and Linkages

10.1 This policy is directly supported by and enforces controls described in the following related policies:

10.1.1 P4 - Access Control Policy: Access to information is governed by classification levels; more sensitive data requires stricter access control and authorization mechanisms.

10.1.2 P11 - User Account and Privilege Management Policy: Reinforces privilege allocation based on need-to-know, which is informed by classification tiers.

10.1.3 P12 - Asset Management Policy: Ensures that each asset in the inventory includes its classification and label, supporting traceability and accountability.

10.1.4 P14 - Data Retention and Disposal Policy: Disposal and retention rules are determined by the classification level of the data and regulatory retention requirements.

10.1.5 P18 - Cryptographic Controls Policy: Applies appropriate encryption standards based on the classification of the information asset.

10.1.6 P22 - Logging and Monitoring Policy: Enables monitoring of access to and movement of classified information, ensuring auditability and detection of mislabeling or misuse.

10.2 Each linkage ensures consistent protection of information across its lifecycle, from creation and classification to secure handling, storage, transmission, and eventual destruction.

11. Reference Standards and Frameworks

11.1 This policy is aligned with internationally recognized standards and regulatory frameworks governing the classification and labeling of sensitive information.

11.2 ISO/IEC 27001

11.2.1 Clause 4.2 - Understanding the Needs and Expectations of Interested Parties. Classification requirements often arise from legal, regulatory, or contractual obligations imposed by interested parties (e.g., GDPR, client NDAs), which must be reflected in the policy.

11.2.2 Clause 6.1.3 - Information Security Risk Treatment. Classification directly affects the selection of risk treatment controls, including access control, encryption, and retention, based on data sensitivity.

11.2.3 Clause 7.2 - Competence. This policy requires personnel responsible for classification and labeling to receive training, which falls under competence requirements.

11.2.4 Clause 7.3 - Awareness. This policy requires all users to be aware of classification tiers and their responsibilities in handling information, aligning with awareness obligations.

11.2.5 Clause 7.5 - Documented Information. This policy is itself a controlled document, and the procedures, training records, and classification labels form part of documented information.

11.2.6 Clause 8.1 - Operational Planning and Control. Classification and labeling are operational processes embedded in data lifecycle management, and this clause ensures that such activities are planned, implemented, and controlled.

11.2.7 Clause 9.1 - Monitoring, Measurement, Analysis and Evaluation. This policy includes provisions for monitoring classification compliance, incident trends, and the effectiveness of the labeling scheme.

11.2.8 Clause 10.1 - Nonconformity and Corrective Action. This policy defines responses to misclassification, including corrective actions such as retraining, updates, and exception handling.

11.3 ISO/IEC 27002:2022

11.3.1 Control 5.12 - Classification of Information. This control ensures that information is classified based on its sensitivity, value, and criticality—precisely what this policy formalizes.

11.3.2 Control 5.13 - Labelling of Information. This control requires appropriate labeling of information in accordance with its classification level, fully addressed in this policy.

11.3.3 Control 5.10 - Acceptable Use of Information and Other Associated Assets. This policy enforces how users must handle classified data, directly supporting acceptable use and preventing misuse.

11.3.4 Control 5.11 - Return of Assets. Classification helps ensure sensitive data is identified and securely returned or sanitized when an employee or vendor departs.

11.3.5 Control 5.9 - Inventory of Information and Other Associated Assets. Classification is often tied to the asset inventory, which must reflect the classification level of each item to support proper control allocation.

11.3.6 Control 5.14 - Information Transfer. Classification levels influence controls on internal and external data transfers (e.g., encryption, approval, access restrictions).

11.3.7 Control 8.12 - Data Leakage Prevention. Enforcing classification and labeling supports the prevention of unauthorized disclosure and data loss.

11.3.8 Control 8.11 - Data Masking. Certain classification levels (e.g., Confidential, Restricted) may require masking when data is used in test, development, or analytics environments.

11.4 NIST SP 800-53 Rev.5

11.4.1 PL-2 - System and Communications Protection Policy and Procedures: Supports classification policies as part of overarching data protection.

11.4.2 AC-16 - Security Attributes: Implements access enforcement based on classification metadata and user permissions.

11.4.3 MP-3 / MP-5 - Media Marking and Transport Protection: Enforces labeling and protection of data at rest and in transit based on classification.

11.5 EU GDPR (2016/679)

11.5.1 Article 5 - Data Protection Principles: Requires personal data to be processed securely and proportionately to its sensitivity.

11.5.2 Article 32 - Security of Processing: Reinforces classification as a mechanism for risk-based data protection and appropriate technical measures.

11.6 EU NIS2 Directive (2022/2555)

11.6.1 Article 21(2)(a): Requires policies for information security and risk management, including asset and data classification controls.

11.6.2 Article 21(3): Encourages adoption of measures to enforce appropriate data handling, supported through classification-based labeling.

11.7 EU DORA (2022/2554)

11.7.1 Article 5 - Governance and Control: Requires governance frameworks that classify data assets for ICT risk control.

11.7.2 Article 9 - ICT Risk Management: Imposes technical and organizational measures for critical ICT assets, including classification and labeling.

11.8 COBIT 2019

11.8.1 DSS05.02 - Manage Security Services: Enforces information security classifications to ensure protection of enterprise data.

11.8.2 MEA03 - Monitor, Evaluate, and Assess Compliance: Supports regular audit and review of classification practices to ensure policy adherence and maturity.